Nile Journals

Nile Journal of Communication & Computer Science

Volume 6, December 2023

Journal Webpage: https://njccs.journals.ekb.eg

Print ISSN: 2805-2366
Online ISSN: 2805-2374

Trends in Biometric Authentication: A review

Rehab M. Ibrahim, Manar M. Elkelany, ARMY AKE team, Magda I. El-Afifi

Nile Higher Institute for Engineering and Technology

Abstract

Data security has come a long way since the inception of passwords and knowledge-based authentication. Due to the constantly growing risk of the spoofing, changing data protection regulations, and company policies, old security measures are no longer viable. The growing need for high security systems that is keeping pace with the development and emergence of the internet of things (IoT) and mobile networks infrastructure that is a breakthrough in connecting anything and all things with each-other, also the appearing of viruses like corona virus. Leads to the need to develop a security system that can work well with the new technologies and also safe on people health so as not to get any viruses. This leads to and initiate the need to the biometric artificial intelligent lockers (AI lockers) to substitute the traditional keys which is easily exposed to lose, stole, damage in any way or even easily copied.

Keywords: Biometric Authentication, Fingerprint, Face Recognition, Iris and handwriting

1. Introduction

Today, one of the safest ways to prevent unauthorised access to digital information is through the use of biometrics. Users can employ biometrics for access control, user login, and other applications that call for user identity verification. Every biometric authentication technique is made to be simple to use while providing high levels of security by verifying that the person using a system or device is who they claim to be.

A security procedure called biometric authentication uses people's distinctive biological traits to confirm they are who they claim they are. Biometric authentication systems match physical characteristics or behavioural patterns to previously authenticated data that is kept in a database. If the biometric information from the two samples agrees, authentication is validated. Access control to physical and digital resources, such as buildings, rooms, and computing equipment, is often managed via biometric authentication. Biometric identification uses biometrics to identify a person, such as fingerprints or retina scans, in contrast to biometric authentication, which uses biometrics to verify that persons are who they claim they are.

2. Overview

The term "biometrics" refers to two very distinct areas of study and application (the ancient Greek words "bios" and "metron" mean "life" and "measure" respectively). The collection, synthesis, analysis, and management of quantitative data on biological communities like forests is the first method, which is the more traditional and is utilised in biological studies, including forestry. It has been studied and used for many generations in relation to biological sciences, and is sometimes just referred to as "biological statistics" [1]. Establishing or certifying something (or someone) as authentic, or that statements made by or about the object are truthful, is known as authentication. The three components of a brief review in this area are Past, Present, and Future

2.1. Past

In China during the 14th century, the European adventurer Joao de Barros noted the first instance of fingerprinting, a type of biometrics. Children's fingerprints were collected by Chinese merchants using ink for identifying purposes. Alphonse Bertillon researched body dimensions and mechanics in 1890 to aid in the identification of offenders. When it misidentified certain people, the police stopped using his Bertillonage method. Richard Edward Henry of Scotland Yard revived the practise of fingerprinting, replacing the Bertillonage technique that had been abruptly abandoned. Early in the 20th century, applied mathematician Karl Pearson attended University College London to study biometric research. He utilised statistical history and correlation to the study of animal evolution and made significant contributions to the science of biometrics. His early work on correlation, the Pearson system of curves, the method of moments, and the chi-squared test.

The military and security services conducted research and developed biometric technology beyond fingerprinting before developing signature biometric authentication processes in the 1960s and 1970s.

2.2. Present

Civil liberties organisations have privacy and identity concerns with the developing and contentious topic of biometric authentication. Biometric industry standards are being evaluated, and legislation and regulations are now being developed. Face identification Although fingerprinting is still the most common kind of biometric identification, ongoing technical advancements and the fear of terrorism will encourage researchers and biometric developers to advance this security technology for the twenty-first century. According to a contemporary perspective, biometric features fall into two categories:

A. Physiological varies from person to person and is tied to the shape of the body. Examples of this form of biometric include fingerprints, face recognition, hand geometry, and iris recognition.

B. Behavioural are connected to a person's behaviour. In this instance, voice, keystroke dynamics, and signature are a few examples. Given that voice differs from person to person, it is occasionally also regarded as a physiological biometric.

A new paradigm has recently emerged that combines human vision with computer databases to create a brain-machine interface. The term "cognitive biometrics" has been used to describe this strategy. Based on certain brain reactions to stimuli that may be used to launch a database search, cognitive biometrics measures cognitive abilities.

2.3. Future

Two services can be provided by a biometric system. Verification is one of them, and authentication is the other. Therefore, the methods employed for biometric authentication need to be rigorous enough to utilise both of these features at once. Cognitive biometrics systems are now being developed to leverage face perception, mental performance, and brain response to odour stimuli for search at ports and high security areas. Other biometric techniques, such as those based on gait (the way a person walks), hand veins, ear canal, facial thermography, DNA, odour and scent, and palm prints, are currently being developed. These biometric technologies may soon provide a defence against the risks facing information security.

Recent study has led researchers to the conclusion that simultaneous authentication and verification methods are the most promising for iris, finger, and palm vein policies. The biggest limitation, though, will be how well the strategy works in actual situations. Therefore, using an artificial system can be a solution in these situations. We've placed a lot of attention on iris detection. We claim that the distance between the pupil and the iris boundary can be calculated following the detection of an iris pattern. Because this characteristic is still distinct for every single person, this metric can be used for recognition purposes. Once more, a man-made system can be created that will update the stored measure when the suggested feature changes for a certain person after a set amount of time.

The manual analysis of the aforementioned procedure yielded a suitable outcome. The rejection ratio for the same person is significantly reduced as a result of the proposed metric's dynamic change. The system is being made viable through the work being done.

3. Who Uses Biometric Authentication?

Biometrics is a convenient way to authorize access to assets or services. The security method has these common use cases:

- Access control
- Online browsing control
- Preventing fraud
- User authentication
- Presence control
- Payment method

Due to its wide range of uses, biometric security benefits many industries, including government agencies, healthcare providers, retailers, hotel chains, and airlines. For example, the military uses biometrics for security purposes on military installations; it also allows soldiers to speed up the security process by using their fingerprints instead of ID cards when entering buildings or going through security checkpoints.

Biometric technology is becoming increasingly prevalent; thus, its applications are growing. Here are some common examples:

- **Border control and immigration.** The US border control subjects arriving and exiting individuals to a biometric screening. It allows CBP officers to identify national security threats and visa overstays.
- **Law enforcement.** Police officers frequently use biometrics to aid criminal investigations. For example, biometric facial identifiers are especially valuable for locating people on watchlists and establishing identities in situations where a person cannot identify themselves.
- **Airport security.** Many major airports have been using biometrics to verify passenger identity. It helps to speed up self-check in time and results in a better passenger boarding experience.
- **Access to mobile devices and authentication.** When electronic identification is necessary, biometric technology adds another layer of security to the process.
- **Banking.** Anti-Money Laundering and Know Your Customer regulations require strong and secure client identification and authentication solutions. By implementing biometric security, banks can prevent fraud, such as identity theft or spoofing.
- **Internet of Things.** Many smart devices use some type of biometrics. For instance, home assistants employ voice as a biometric identifier.

4. Biometric Authentication Technologies

Biometric security systems, also known as modalities, are built to recognize different biometric traits during authentication. Each biometric system involves unique biological and behavioural aspects. The biometric traits implemented in a system have an effect on its performance. Thus, it’s important to get familiar with the most common types.

4.1 Face Recognition technology

One of the most frequently employed biometric features is the human face. It is the method of biometric identification that is the most natural [2]. With the help of still or moving face photos, verification is made easier. The location, shape, and spatial relationships of a person's eyes, nose, mouth, and other facial features are all mapped out using artificial intelligence (AI) during the process. The technology helps find a face amid a vast number of existing images and assesses whether two distinct shots of the same individual are identical.

The production of the precise facial features required for facial metric technology is illustrated in Figures 1 and 2.
The system typically looks for the placement of the eyes, nose, and mouth as well as
the distances between these features.

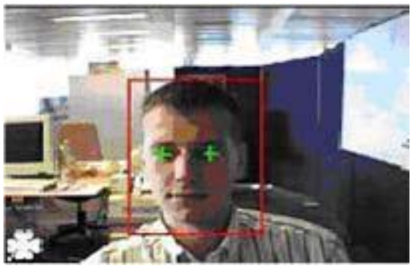

Fig. 1 Recognition of face from Body

The face region is resized to a predetermined set size, such as 150–100 points. The canonical image is referred to as this normalised facial image. Following that, a face template is created and the facial metrics are calculated. There are systems with templates as small as 96 bytes, while the normal size of such a template is between 3 and 5 KB. Below is a figure for the normalised face.

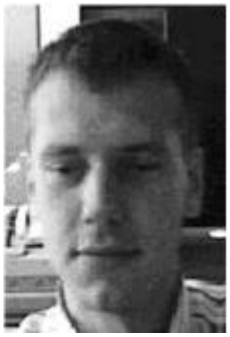

Fig. 2 Normalized Face

The Eigen Face technique (Fig. 3) categorises faces based on its degree using a predetermined set of 100–150 eigen faces. The resulting eigen faces will manifest as a pattern of alternately light and dark regions. This design demonstrates how various facial features can be highlighted. It needs to be assessed and graded. A pattern will be present to assess symmetry, the presence of facial hair, the location of the hairline, and the size of the nose and mouth. Other eigen faces feature patterns that are harder to spot, and their images may not even closely resemble human faces. The portrait-making approach used by the police is actually identical to this one, but the image processing is automated and based on a real photo. Only the 40 template eigen faces with the highest degree of fit are required to rebuild the face with a 99.9% accuracy. Each of the 150 eigen faces is given a degree of fit. Software for facial recognition is used throughout [3]–[6].

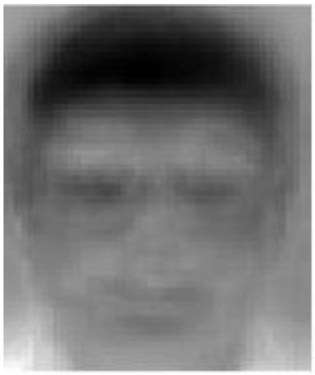

Fig. 3 Eigen Face

Benefits of Facial Recognition

Systems that recognise faces have an advantage over other biometrics. The maximum level of security is demonstrated by this biometric modality when combined with liveness detection, thermal imaging, and other technology.

Face recognition technology makes it possible to quickly and effectively identify returning users by detecting numerous spoof artefacts, such as screens, pictures, masks, etc.

Facial recognition is also incredibly simple to utilise. This biometric modality can be used with the aid of a user's phone because cameras have become such an integral part of our life. The face is the most chosen biometric characteristic for authentication as a result.

Typical Obstacles to Facial Recognition

Users may run into a number of problems while using facial recognition for authentication. The first is a video or image's inappropriate background. A person's face may be impossible to identify against a complicated background, hindering successful authentication. Lighting presents another difficulty. Poor lighting may cause the process to fail. It's also important to remember that a face can alter significantly with time. Ageing, cosmetic surgery, accidents, and illness are frequent causes.

4.2 Voice Technology

A biometric characteristic called voice combines biological and behavioural characteristics. Many physical traits, such as the size and shape of a person's mouth, tongue, nose, or vocal cords, affect the sound of their voice. Their emotions, health conditions, or language can all have a big impact.

A person can be recognised by their voice using voice or speaker recognition. Simple speaking activities are given to speakers in order to develop a distinctive voice profile. The technology then compares the profile to fresh voice samples used to confirm the speaker's identity.

A person's voice is distinctive and very difficult to imitate. Voice recognition can also be easily put into use. Users typically utilise their phones and are not required to own any additional equipment. Common Challenges of Voice Recognition. A speaker recognition system may fail for a number of significant reasons. Any respiratory condition, like the common cold, can readily change the user's voice, making authentication impossible. The process could potentially be hampered by ambient noise.

4.3 Fingerprints Technology

The use of fingerprints in forensics is no longer limited to them. The majority of individuals utilise fingerprint biometrics these days. Owners can use their fingerprint to gain secure access to their devices because it is simple to deploy in any device, including a laptop or mobile phone. Figure 4 depicts the finger print obtained using an optical fingerprint reader. Safe access to their devices. The finger print obtained from an Optical Fingerprint Reader is shown in Fig. 4.

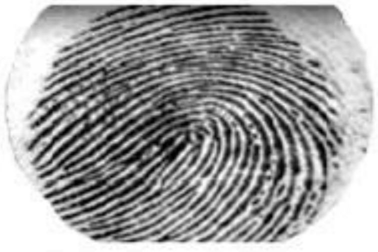

Fig. 4Fingerprint Bitmap

The optical finger is approximately 10*10*15 in size. It is challenging to reduce them more since the reader must take into account the source of the light sensor and the light reflecting surface. The capacitance of the finger is the foundation of the optical silicon fingerprint sensor. A silicon chip with rectangular arrays of capacitors makes up a dc-capacitive finger print sensor. When placing a finger against a chip's surface, the finger print's ridges are adjacent to the neighbouring pixels and have a high capacitance to them. The other plate of the capacitors contains a tiny area of metallization on the chip surfaces. The valleys have lower capacitance because the pixels closest to them are farther away from them.

The newest and least prevalent fingerprint type is ultrasound. The user places the finger on a piece of glass using ultrasound to scan the figure surfaces, and the ultrasonic sensor moves and reads the entire finger print. It takes a moment or two to do this.

Techniques for matching fingerprints fall into two groups. One of them is correlation-based, while the other is minutiae-based. By first locating the minutiae points, minutiae-based approaches can then map their relationship placement on the finger. Image translation and rotation have an impact on correlation-based approaches, which need on a precise location for a registration point [4], [7], [8].

Advantages of fingerprint identification

The fact that each person's fingerprint is unique is the main benefit of fingerprint scanning. Even identical twins' fingerprint ridges and patterns differ.

The simplicity of usage and accessibility are other advantages. Even while they are extensively used and installed in consumer electronics, such as laptops and door locks, a standalone fingerprint scanner is also simple to acquire.

Typical Obstacles to Fingerprint Recognition

Systems using fingerprints for authentication have drawbacks despite their advantages. Fraudsters have developed techniques for fabricating fingerprints and using them for illegal purposes. Even though getting around fingerprint-based security is difficult, it is doable with enough effort. Additionally, whether a person is unconscious or asleep, it is still possible to carry out unauthorised authentication.

4.4 Iris Technology

Iris, a coloured, circular membrane surrounding the pupil of the human eye is another unique trait. The complex structure of the iris is extremely hard to replicate. Thus, it is also used in biometric systems Iris patterns are distinctive and can be captured using a technique for video-based picture acquisition. Each iris structure has a unique, intricate pattern. The corona, crypts, filaments, freckles, pits, furrows, striations, and rings are only a few examples of the distinctive features that can be present [9]. Fig. 5 displays an Iris picture.

Fig. 5. Image of IRIS

A specialised grey scale camera is used to capture the iris pattern from a distance of 10 to 40 cm. The software then attempts to identify the iris in the resulting grayscale image of the eye. If an iris is discovered, the software builds a net of curves to cover it. The software generates the iris code based on the darkness of the points along the lines. Here, two factors need to be considered. First, the lighting condition affects the overall darkness of the image, therefore the threshold used to determine whether a given location is dark or bright cannot be static; it must be computed dynamically in accordance with the overall picture darkness. Second, as the pupil's size varies, so does the iris's size. An appropriate transformation must be performed prior to computing the iris code.

The decision-making procedure uses two iris codes from which the matching software computes the hamming distance based on the variety of bits. The security threshold is compared to the hamming distance score (within the range, 0 denotes the same iris codes) before the final determination is made. Because it just counts the bits in the exclusive OR of two iris codes, computing the hamming distance of two iris codes is very quick. With this method, we can also use the idea of template matching. In template matching, a statistical comparison between a produced and a stored iris template is made. Decisions are made in accordance with the outcome [8], [10]

Iris Recognition's advantages

Iris is an organ that may be seen from the outside and is well protected from harm. It is simple to use and configure for authentication. Additionally, altering pupil size may help to maintain liveliness.

Challenges of Iris Recognition

Despite its benefits, the iris scanners are still a developing technology. Even though it seems promising, current systems have a high false non-match rate (FNMR).

4.5 Handwriting Technologies

Similarly, to optical character recognition (OCR), handwriting recognition is capable of using pattern matching for converting handwritten letters into computer text. However, handwriting is more or less unique to a person, consequently, it is also a behavioural biometric system.

You can have static or dynamic technologies. The handwriting is merely compared in the static procedure. On the other hand, the dynamic method examines a user's writing speed, form, pen pressure, stroke, and other features to confirm their identification. Typing recognition helps in digital text imputation by speeding up the process.

Handwriting Recognition's Advantages

Users can easily and intuitively comprehend handwriting recognition. The procedure' security is increased when the likelihood of forged handwriting is reduced.

Handwriting Recognition Issues

Our handwriting is distinctive, but it's also very inconsistent. Numerous causes, such as stress, weariness, emotional state, or injury, might cause a person's writing to change. Because of this, handwriting offers a minimal level of security.

4.6 Technology for Hand Geometry

It is based on the observations that almost everyone has a unique hand form and that, after a certain age, this shape does not change. These methods involve estimating the hand's length, width, thickness, and surface area. The hands can be measured using mechanical or optical principles [11], [12].

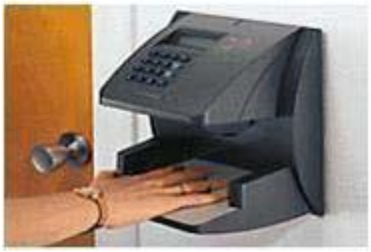

Fig. 6. Scanner for hand geometry

The two subcategories of optical scanners are as follows. The first type of devices produce a bitmap image of the contour of the hand in black and white. A black and white camera and a light source make this task simple. The computer software processes the bitmap image. In this situation, only the hand's 2D properties can be applied. Other categories of hand geometry systems are more difficult. They have two (vertical and horizontal) sensors for measuring the hand's shape and employ specific guide marking to properly segment the hand. As a result, all 3D feature data is handled by sensors in this category [4], [13]. Figures 6 and 7 depict the system for measuring hands. Some hand geometry scanners solely create video signals of the hands when scanning hands. The appropriate video or image of the hand is subsequently obtained using the computer's image digitalization and processing [13].

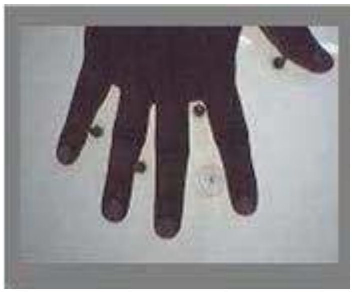

Fig. 7 Acquired Hand Image

4.7 Technology for Retinal Geometry

As the blood vessels at the back of the eye have a distinct pattern from eye to eye and person to person (Fig. 8), it is dependent on the blood vessel pattern in the retina of the eye. Since the retina cannot be seen directly, it must be illuminated by a source of coherent infrared light. The blood vessels in the retina absorb infrared energy more quickly than the surrounding tissue. The retina blood vessel pattern image is next examined.

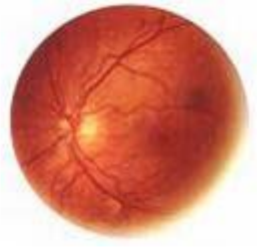

Fig. 8 Picture of a retina

For retina scans, the patient must take off their spectacles, position their eye close to the scanner, fix their gaze on a predetermined point for 10 to 15 seconds while the scan is being performed. A low-intensity coherent light source is projected onto the retina during a retinal scan in order to illuminate the blood vessels, which are subsequently captured on camera and evaluated. To read the blood vessel patterns, a coupler is employed. Since it is currently impossible to fabricate a human retina, a retina scan cannot be falsified. Furthermore, a deceased person's retina degrades too quickly to fool a retinal scan. Compared to fingerprint identification errors, which can occasionally reach 1 in 500, retinal scan errors have a frequency of 1 in 10,000,000 [14].

4.8 Technique for Speaker Recognition

Because each person's voice has a unique pitch, voice is also a physiological property. However, voice recognition is primarily reliant on the analysis of a speaker's behavioural characteristics.

The acoustic characteristics of speech that have been shown to vary between persons are used in speaker recognition. These auditory patterns reflect both acquired behavioural patterns and anatomy (such as the size and shape of the throat and mouth). (For instance, speaking style and voice pitch) [15], [16].

The three spoken input styles used by speaker recognition systems are given below.

a) Text-based.

b) Text-prompted.

c) Text-unrelated

Text-dependent technology includes choosing and enrolling one or more voice passwords. Every time there is a worry about imposters, text prompts are used. Hidden Markov models, pattern matching algorithms, neural networks, metric representation, and decision trees are just a few of the many technologies utilised to process and store voice prints. Technology sometimes employs "anti maker" strategies like cohort models and global models.

Age-related voice alterations must also be taken into account by recognition systems. The biometrics’ collection is regarded as non-intrusive. By utilising already-existing microphones and audio transmission technologies, the system allows for recognition over large distances using regular telephones (wire line or wishes) [17].

4.9 Other Methods

Below is a description of some other biometric authentication methods that are currently in use.

I. **Palmprint:** A slightly different fingerprint technology use is palmprint verification. Although palmprint scanning uses optical readers very similar to those used for fingerprint scanning, their size is substantially larger, which makes it difficult to use them in workstations or portable devices.

II. **Hand Vein:** The geometry of the hand veins is based on the fact that each person's vein pattern is unique. An infrared camera's image of the hand shows a darker pattern due to the veins under the skin's absorption of infrared light. Research and development are still ongoing for the hand vein geometry. British Technology Group is a manufacturer of one such system. The device is known as Veincheck and employs a template that is 50 bytes in size [17]–[19].

I. **DNA:** Currently, DNA testing requires a body sample, such as tissue, blood, or another bodily fluid. This capturing technique still requires improvement. The DNA analysis has not yet advanced to the point of being considered a biometric technology. In just ten minutes, human DNA may now be analysed. The significance of DNA matching could increase as soon as technology develops to the point where it can be done automatically and in real time. Because of its current stronghold in crime detection, Biometric Systems DNA will for the time being remain in the realm of law enforcement [8], [17].

II. **II. Thermal imaging:** The hand vein anatomy can be compared to this technology. The vein pattern in the face or wrist can likewise be visualised using an infrared light source and camera [20].

III. **III. Ear Shape:** When ear markings are discovered at crime scenes, law enforcement applications employ ear shapes to identify people. It remains to be seen if this technology will advance to applications for access control. The French business ART Techniques manufactures an ear shape verifier called the Octophone. It has cameras that take two photos of the ear and a lighting unit inside of a telephone-style handset [17]**.**

IV. **Body Odor:** The biometrics for measuring body odour are founded on the idea that almost every human smell is distinctive. The smell is picked up by sensors that can pick up the scent from non-intrusive body parts, such the back of the hand. Mastiff Electronic Systems is investigating ways to record a person's odour. Volatile compounds make up each individual human odour. The system extracts them and turns them into a template. The privacy concern is raised by the usage of body odour sensors since the odour of the body contains a lot of delicate personal data. By examining the body odour, it is possible to determine various illnesses or recent activities (such as sex, for example) [17], [21].

V. **Dynamics of Keystroke:** Keystroke dynamics is a technique for identifying someone by their typing rhythm that works with both professional and beginner two-finger typists. Systems can check the user's identity during the login process or they can keep an eye on the Biometric Systems 32 typist all the time. Since only a software package is required, installing these systems should be inexpensive [22].

VI. **Fingernail Bed:** The US business AIMS is working on a technology that detects the skin tissue just below the fingernail. Nearly parallel rows of vascularly dense skin make up its tongue-and-groove structure. The AIMS system measures the space between these parallel dermal structures, which are separated by tiny channels.

5. Which Type of Biometric Authentication is Best?

As you can see, the uses and security of each biometric authentication technique differ. This does not imply that the less secure solutions are worthless, either. Everything depends on the goal and usability. For instance, if a home assistant switched from speech recognition to facial recognition, it would be impossible for users to issue commands. On the other hand, a banking app that incorporates facial recognition technology can assist in rapidly and securely authenticating a customer.

6. Conclusion

The future of authentication is biometrics. The system provides a more convenient, cost-efficient, and secure way to confirm identities. Comparing biometric systems to conventional password-based ones has various benefits. Since it cannot be lost or stolen like passwords, it offers a higher level of protection, making it more challenging for hackers to get access. When used in conjunction with other security measures like two-factor authentication and encryption, biometrics also lowers the danger of identity theft.

References

[1] U. M. D. E. C. D. E. Los, “Identity and Smart Card Technology and Application Glossary,” 2007.

[2] M. A. Dabbah, W. L. Woo, and S. S. Dlay, “Secure authentication for face recognition,” *Proc. 2007 IEEE Symp. Comput. Intell. Image Signal Process. CIISP 2007*, no. November 2014, pp. 121–126, 2007, doi: 10.1109/CIISP.2007.369304.

[3] A. A. Ross and R. Govindarajan, “Feature level fusion of hand and face biometrics,” *Biometric Technol. Hum. Identif. II*, vol. 5779, no. March, p. 196, 2005, doi: 10.1117/12.606093.

[4] L. Hong and A. Jain, “Integrating faces and fingerprints for personal identification,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 1351, no. 12, pp. 16–23, 1997, doi: 10.1007/3-540-63930-6_99.

[5] A. K. Jain, “Handbook of Face Recognition,” pp. 1–40, 2014, [Online]. Available: papers3://publication/uuid/17FEF3DC-D6F9-408B-96E5-871ED133A4F1.

[6] F. Cardinaux, C. Sanderson, and S. Bengio, “User authentication via adapted statistical models of face images,” *IEEE Trans. Signal Process.*, vol. 54, no. 1, pp. 361–373, 2006, doi: 10.1109/TSP.2005.861075.

[7] R. Cappelli, D. Maio, D. Maltoni, J. L. Wayman, and A. K. Jain, “Performance evaluation of fingerprint verification systems,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 28, no. 1, pp. 3–17, 2006, doi: 10.1109/TPAMI.2006.20.

[8] A. K. Jain, A. Ross, and S. Pankanti, “Biometrics: A tool for information security,” *IEEE Trans. Inf. Forensics Secur.*, vol. 1, no. 2, pp. 125–143, 2006, doi: 10.1109/TIFS.2006.873653.

[9] N. Jindal and V. Sawhney, “Iris Recognition : an Emerging Biometric Approach,” *Ieeexplore.Ieee.Org*, vol. 1, no. 2, pp. 203–207, 1997, [Online]. Available: https://ieeexplore.ieee.org/abstract/document/628669/.

[10] J. Daugman, “The importance of being random: Statistical principles of iris recognition,” *Pattern Recognit.*, vol. 36, no. 2, pp. 279–291, 2003, doi: 10.1016/S0031-3203(02)00030-4.

[11] V. Kanhangad and A. Kumar, “Personal verification from the geometry of human hands,” *Adv. Top. Biometrics*, pp. 247–261, 2011, doi: 10.1142/9789814287852_0010.

[12] E. Kukula and S. Elliott, “Implementation of hand geometry at purdue university’s recreational center: An analysis of user perspectives and system performance,” *Proc. - Int. Carnahan Conf. Secur. Technol.*, pp. 83–88, 2005, doi: 10.1109/ccst.2005.1594879.

[13] C. Sanchez-avila and A. Gonzalez-marcos, “Biometric identification through hand geometry measurements,” vol. 22, no. 10, pp. 1168–1171, 2000.

[14] T. Chihaoui, H. Jlassi, R. Kachouri, K. Hamrouni, and M. Akil, “Personal authentication using digital retinal images,” *13th Int. Multi-Conference Syst. Signals Devices, SSD 2016*, pp. 280–286, 2016, doi: 10.1109/SSD.2016.7473709.

[15] B. Kar, B. Kartik, and P. K. Dutta, “Speech and Face Biometric for Person Authentication,” pp. 391–396, 2006.

[16] A. Eriksson and P. Wretling, “How flexible is the human voice ? A case study of mimicry HOW FLEXIBLE IS THE HUMAN VOICE ? – A CASE STUDY OF MIMICRY .,” no. September 1997, pp. 1–5, 2015, doi: 10.21437/Eurospeech.1997-363.

[17] A. K. Jain, A. Ross, and S. Prabhakar, “An Introduction to Biometric Recognition,” vol. 14, no. 1, pp. 4–20, 2004.

[18] S. Im, H. Park, Y. Kim, S. Han, S. Kim, and C. Kang, “An Biometric Identification System by Extracting Hand Vein Patterns,” vol. 38, no. 3, pp. 268–272, 2001.

[19] A. Kumar, D. C. M. Wong, H. C. Shen, and A. K. Jain, “Personal Verification Using Palmprint and Hand Geometry Biometric,” pp. 668–678, 2003.

[20] C. Lin and K. Fan, “Biometric Verification Using Thermal Images of Palm-Dorsa Vein Patterns,” vol. 14, no. 2, pp. 199–213, 2004.

[21] P. Inbavalli and G. Nandhini, “Body Odor as a Biometric Authentication,” vol. 5, no. 5, pp. 6270–6274, 2014.

[22] Lien, Chi-Wei, and S. Vhaduri. "Challenges and Opportunities of Biometric User Authentication in the Age of IoT: A Survey." *ACM Computing Surveys*, 2023.